IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
DEL RIO DIVISION

The State of Texas, *Plaintiff,*	)	
v.	)	No. DR-23-CV-00055-AM
Alejandro Mayorkas, *et al.*, *Defendants.*	)	

DECLARATION OF ELAINE DISMUKE

I, Elaine Dismuke, pursuant to 28 U.S.C. § 1746, based upon my personal knowledge and information made known to me in the course of my employment, hereby declare as follows, relating to the above-captioned matter:

1. I am currently the eDiscovery Team Lead, eDiscovery Team, Enterprise Infrastructure Operations Directorate, Office of Information and Technology ("OIT") Enterprise Services, U.S. Customs and Border Protection ("CBP"). I have held this position since January 2011.

2. I graduated from the University of Maryland in 1973 with a Bachelor of Science in Biology and was ITIL® certified in 2006. My specialized training includes, but is not limited to: Certified Information Systems Auditor (CISA) Training in 2016, Clearwell Admin. Training in 2014, Exchange 2007 Server Training in 2009, Exchange 2003 Server training in 2007, ITIL Foundations, Version 3 in 2008, Implementing and Managing MS Server with Exchange Server in 2003, Basic Outlook/Exchange Support in 2006, Lotus 6 Administration – Server and User Support Training in 2005, Lotus R5 training in 2005, Cc:Mail Administration and User Support in 1998, and Softswitch –mainframe training in 1998.

3. My program office, referred to as "the OIT eDiscovery Team," is responsible for, among other things, searching for and collecting certain electronically stored information ("ESI") for CBP and its subcomponents. As the eDiscovery Team Lead, I oversee the work of six CBP employees and employee contractors. I am trained to search for and collect ESI from certain locations, as are my six colleagues.

4. I am familiar with the above-captioned case as CBP's Office of Chief Counsel recently requested that the OIT eDiscovery Team search for and collect ESI for the case.

Collection of Electronically Stored Information Using Microsoft Purview

5. The OIT eDiscovery Team can only search for and collect ESI stored in two locations: Exchange Mailboxes and SharePoint. Exchange Mailboxes houses Microsoft Outlook, which includes emails, their attachments, calendar entries, and most types of Microsoft Teams chats. SharePoint houses OneDrive (a SharePoint file library), traditional SharePoint sites, and Microsoft Teams sites. This does not include all ESI that may be stored in the many databases and systems of record used by CBP.

6. The OIT eDiscovery Team uses Microsoft Purview—a program for governing and securing data—to search for and collect ESI from these two locations. The process is often complex, laborious, and time consuming.

7. To conduct a search for ESI stored in Exchange Mailboxes, the OIT eDiscovery Team must first search for each custodian's name individually in Microsoft Purview and select the custodian for inclusion.

8. To conduct a search for ESI stored in SharePoint, the OIT eDiscovery Team must gather Uniform Resource Locators (URLs) of the precise locations to be searched. If the search includes OneDrive, the OIT eDiscovery Team must search CBP's instance of Active Directory.

Active Directory is a Microsoft service that provides centralized authentication and authorization to network resources. In Active Directory, the OIT eDiscovery Team identifies each custodian's Personal Identity Verification (PIV) account number. The OIT eDiscovery Team then manually enters each custodian's PIV account number in Microsoft Purview to identify and select the URL associated with each custodian's OneDrive account. If the search includes traditional SharePoint sites or Teams channels, the OIT eDiscovery Team must request and procure a report from OIT's O365 Team for identifying information associated with each of the applicable SharePoint sites/Teams channels. The OIT eDiscovery Team must then manually enter that information in Microsoft Purview.

9. With this starting information, the OIT eDiscovery Team then enters remaining search parameters into Microsoft Purview, namely, any applicable date range, *e.g.*, January 1, 2023 through January 31, 2023, and keyword query, *e.g.*, *"hat" AND "car" AND "bag"*. As the foregoing example illustrates, a single keyword query can include Boolean connectors, *i.e.*, "AND," "OR," or "NOT"; however, it cannot exceed 20 keywords including any such Boolean connectors. As such, the keyword query *"hat" AND "car" AND "bag"* would consist of five of the maximum 20 keywords. Although the OIT eDiscovery Team can conduct multiple keyword queries at one time, they can only run those queries against a single date range and the total number of keywords in those queries must not exceed 20 keywords.

10. When the OIT eDiscovery Team receives requests to run keyword queries that exceed 20 keywords—a commonplace occurrence—the OIT eDiscovery Team must break up those keyword queries so that each one is 20 keywords or fewer and then reenter the information described in Paragraphs 7 and 8 in Microsoft Purview for each of those broken-down keyword queries. This burden is often compounded by the number of Exchange Mailboxes and

SharePoint locations that need to be selected or enumerated, respectively. In my experience, setting up even a relatively simple search—for instance, one single search for two keywords across two custodians' Exchange Mailboxes during a two-year period—takes approximately 30-45 minutes.

11. The time each search takes to complete—meaning for Microsoft Purview to run and finish the search and return a report of the results—varies based on the scope and details of the search, but frequently takes days. Specific factors include the search's complexity, *e.g.*, the extent to which it incorporates phrases rather than simple keywords; the prevalence of the search terms in the search locations; the number of custodians; and the data parameters. The bandwidth of CBP's Microsoft Purview instance is also relevant. The OIT eDiscovery Team shares CBP's Microsoft Purview with CBP's Cyber Security Directorate, Cyber Defense Forensic Team, and the higher the number of contemporaneous searches, the slower the throughput.

12. Once a search is complete, the OIT eDiscovery Team exports the resulting data from Microsoft Purview. This is a two-step process: First, the OIT eDiscovery Team exports the data to a .pst file in Purview. Second, the OIT eDiscovery Team downloads that .pst file from Purview to a server.

13. The OIT eDiscovery Team can, theoretically, run a CBP-wide search across ESI stored in Exchange Mailboxes and SharePoint sites. Such searches may collect sizeable amounts of data, however, rendering them extraordinarily if not prohibitively burdensome to administer. Specifically, CBP is limited to exporting 2 terabytes of data from Microsoft Purview per day. Once CBP reaches that 2 terabyte per day limit, CBP, including the OIT eDiscovery Team, is unable to export any additional data from Microsoft Purview until 00:00 UTC. Further, due to Microsoft Purview's limitations, the OIT eDiscovery Team is unable break up the results of a

search for exporting. Accordingly, when a search returns more than 2 terabytes of data, the OIT eDiscovery Team must break up the original search into searches designed to collect smaller amounts of data—each collecting less than 2 terabytes of data—and run each of those sub-searches.

Open Cases

14. Currently, the eDiscovery Team has 125 open cases in various stages of production and review. These cases are based on civil litigation requests, trade issues, congressional fact finding, criminal cases, and Freedom of Information Act (FOIA) requests. Those requests come from the Office of Chief Counsel, the Office of Professional Responsibility, the CBP FOIA Office, the Department of Homeland-Office of Inspector General, the SOC (Security Operations Center), and Managerial Administrative requests. This figure does not include the requests from OIT's Technology Service Desk for individual email message restores, nor does this figure include requests sent to the OIT eDiscovery team from the CBP Email Services team, the Office 365 Project team, or one of our customers asking for additional data their previously completed request. Data pulls range from a single search to searches on 30 or more custodians with or without key words using multiple key words. There is no way to know how much data will be included in each search case until that search is pulled. Search time frames have been as short as 1 day to as long as 11 years.

The Instant Litigation

15. As referenced in Paragraph 4, on November 9, 2023, the OIT eDiscovery Team conducted an ESI search and collection in this case. Specifically, the OIT eDiscovery Team searched seven custodians' email and OneDrive accounts for ESI, created during a 32-month period, containing any of ten terms:

CBP Officials	**Date Range**	**Search Terms**
David BeMiller Chief, Law Enforcement Operations Headquarters	March 6, 2021 through November 9, 2023	Barrier Wire Impediments Concertina Lock Fence Gate Razor C-wire Impede
Juan Bernal (Acting) Chief Patrol Agent Del Rio Sector		
Milton Moreno (Acting) Deputy Chief Patrol Agent Del Rio Sector		
Micky Donaldson Patrol Agent in Charge Eagle Pass North Station		
George Cavazos Deputy Patrol Agent in Charge Eagle Pass North Station		
Gerardo Inocencio Patrol Agent in Charge Eagle Pass South Station		
Mario Trevino, Jr. Deputy Patrol Agent in Charge Eagle Pass South Station		

16. Following de-duplication in Microsoft Purview, the search returned 156,704 emails from Microsoft Outlook, many of which had attachments, and 695 standalone documents from Microsoft OneDrive. These emails with their attachments combined with the standalone documents totaled 153.2 gigabytes.

17. Assuming these results explained in Paragraph 16 to be representative, if this same search were to be run against 100 custodians, with the same search parameters—meaning limited to their emails and OneDrive files—and with the same ten search terms, I estimate that it would return approximately 2,188 gigabytes, or 2.188 terabytes, of data. With the same assumption and parameters, if this search were to be run against 1,500 custodians, I estimate that it would return

approximately 32,820 gigabytes, or 32.82 terabytes, of data. With the same assumption and parameters, if this search were to be run against 60,000 custodians, I estimate that it would return approximately 1,312,800 gigabytes, or 1,312.8 terabytes, or 1.3128 petabytes, of data.

18. As described in Paragraph 13, the OIT eDiscovery Team is unable to break up retrieved data to export batches under the 2 terabyte per day limit. Accordingly, to run any of the three searches described in Paragraph 17, the OIT eDiscovery Team would need to break the search into chunks, likely corresponding to specific time periods which, together, would encompass the entire 32-month period.

a. If the search were limited to 100 custodians and resulted in 2.188 terabytes of data, the search would need to be broken up into at least two sub-searches, each returning 2 terabytes or less of information. Put another way, the OIT eDiscovery Team would need to set up and run one of these sub-searches a day for at least two days to search for and collect the aggregate data. During that time, the OIT eDiscovery Team would be unable to use Microsoft Purview for the dozens of other open matters described in Paragraph 14; many such matters relate to other federal litigation. Additionally, CBP's Cyber Security Directorate, Cyber Defense Forensic Team would be unable to use Microsoft Purview for their internal investigations, as described in Paragraph 11.

b. If the search were limited to 1,500 custodians and resulted in 32.82 terabytes of data, the search would need to be broken up into at least 17 sub-searches, each returning 2 terabytes or less of information. Put another way, the OIT eDiscovery Team would need to set up and run one of these sub-searches a day for at least 17 days to search for and collect the aggregate data. During that time, the OIT eDiscovery Team would be unable to use Microsoft Purview for the dozens of other open matters described in Paragraph 14; many such matters

relate to other federal litigation. Additionally, CBP's Cyber Security Directorate, Cyber Defense Forensic Team would be unable to use Microsoft Purview for their internal investigations, as described in Paragraph 11.

b. If the search were run against 60,000 custodians and returned approximately 1,312.8 terabytes of data, the search would need to be broken up into at least 657 sub-searches, each returning 2 terabytes or less of information. Put another way, the OIT eDiscovery Team would need to set up and run one of these sub-searches a day for at least 657 days, or over two years, counting weekends, to search for and collect the aggregate data. During that time, the OIT eDiscovery Team would be unable to use Microsoft Purview for the dozens of other open matters described in Paragraph 14; many such matters relate to other federal litigation. Additionally, CBP's Cyber Security Directorate, Cyber Defense Forensic Team would be unable to use Microsoft Purview for their internal investigations, as described in Paragraph 11.

Collection of Electronically Stored Information Using Other Means

19. As described in Paragraph 5, the OIT eDiscovery Team is only able to search for and collect certain ESI stored in locations, primarily associated with Microsoft. The OIT eDiscovery Team does not have the capability to search for and collect other ESI, such as information on cell phones and contained in noncustodial sources.

Ingestion of Electronically Stored Information into RelativityOne

20. The OIT eDiscovery Team generally uploads collected ESI—whether information that OIT eDiscovery Team has collected using Microsoft Purview or that CBP subcomponents have themselves collected—to CBP Office of Chief Counsel's instance of RelativityOne. RelativityOne is a cloud-based document review platform. To do so, the OIT eDiscovery Team must move the collection to a server and then upload it to RelativityOne's processing module, a

process known as “staging.” Staging takes time, especially the uploading portion, where CBP is at the mercy of RelativityOne’s bandwidth.

I declare, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed this 20 day of November, 2023.

ELAINE R DISMUKE

Digitally signed by ELAINE R DISMUKE
Date: 2023.11.20 18:59:17 -05'00'

Elaine Dismuke
eDiscovery Team Lead
Enterprise Infrastructure Operations Directorate
Office of Information Technology
Enterprise Services
U.S. Customs and Border Protection